ADOA

HRIS – Human Resources Information Solution

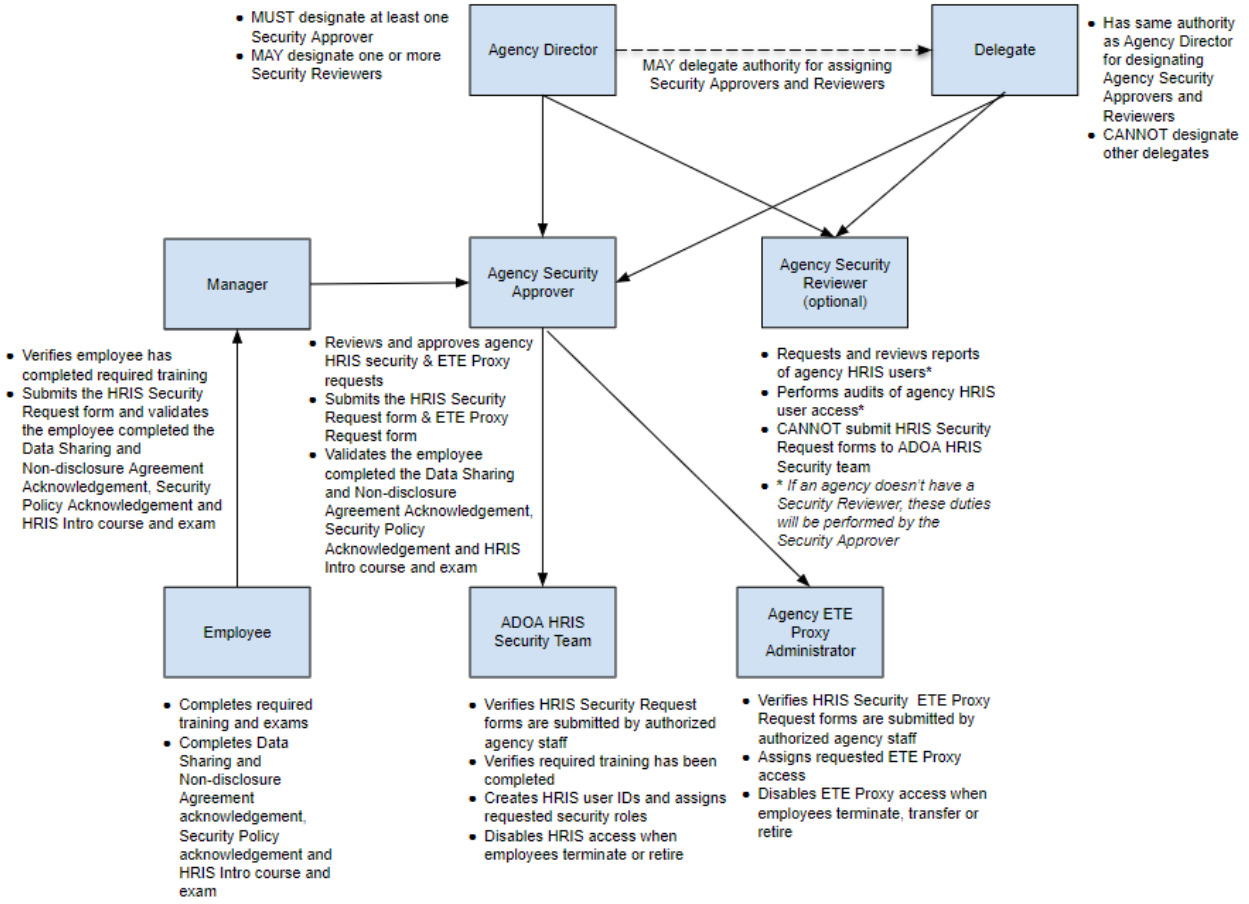
Resource Guide:

HRIS Security Administration Policy

HRIS Security Administration Policy

Table of Contents

HRIS Security Administration Roles and Responsibilities



Introduction

HRIS security is the joint responsibility of each agency and the Department of Administration. Security is a critical component of all automated or manual Financial and Human Resource systems. Proper separation of duties and security measures must be present.

Internal control policies that have already been established for the State should be reviewed and considered. The relevant policies can be found here: **http://www.gao.az.gov/publications/SAAM**.

HRIS security access is role based. The HRIS team has established a number of security roles that closely coincide with the various functions in the areas of HR, Payroll, Benefits and Finance that an agency performs. These security roles are generic in nature and should apply to all agencies. Each HRIS user must be associated with at least one security role. Once the security role(s) is determined, the HRIS Security team will be able to grant access to HRIS data, forms and reports needed to perform that role. A list of current HRIS security roles can be viewed at the HRIS website: https://hr.az.gov/content/securityrolesandtraining

Idle Accounts

According to Arizona Statewide Information Security Policy, Section 6.7 and its subsections address the criteria for inactive accounts. If a system contains "Personally Identifiable Information" the standard is to disable the account after no more than 90 days of inactivity.

In general, users are expected to be active users of HRIS to maintain Power User access. If an account is found to be inactive, the account will be **deleted** without notice. Inactivity is defined as:

- Not logging into HRIS for at least 90 days

Users may choose to remove their Power User account at any time by submitting a Power User request form with the action reason of “Remove all HRIS access”. To reactivate a **deleted** account, a new Power User form will need to be submitted using the action reason “Reinstate/Rehire/Agency Transfer”.

Agency HRIS Security Administration Roles and Responsibilities

Compute Week is defined as the week the State Employees are paid.

The payroll compute runs on Tuesday evening. During this time, access is restricted to view only.

- Update access will be turned off at 2:00 pm on Tuesday of the compute week.

Following the Tuesday evening compute, regular access to the system resumes, typically at 6:00 am Wednesday morning.

Each agency is responsible for ensuring the correct HRIS security roles are assigned to its

employees. The positions and related HRIS security administration responsibilities are outlined below.

Agency Directors

1. Responsible for creating the control environment at the agency
2. Responsible for ensuring that internal controls are adhered to at the agency
3. Should have familiarity with HRIS as well as general knowledge of Human Resources, Benefits and Payroll operations at the agency
4. Responsible for designating HRIS Security Approvers for the agency
    - The Agency Director SHALL designate at least one employee to be authorized as an Agency Security Approver to review and approve all of the agency’s user access to HRIS
    - If no Security Approver is designated, the role of Agency Security Approver is assumed by the Agency Director
    - It is highly recommended that more than one Agency Security Approver is designated to

ensure continuity of operations

- Shall carefully review the qualifications of an employee who they wish to make the Agency Security Approver
- Shall review the requirements and responsibilities of the Agency Security Approver listed below

5. Responsible for removing an Agency Security Approver if they separate from State service or have a change in employment where acting as the Agency Security Approver is no longer appropriate
6. Responsible for designating Agency Security Reviewers for the agency
    - The Agency Director MAY designate an employee to act as the Agency Security Reviewer to assist with managing HRIS access for its employees
    - Shall carefully review the qualifications of an employee who they wish to make the Agency Security Reviewer
    - Shall review the requirements and responsibilities of the Agency Security Reviewer listed below
7. Responsible for removing an Agency Security Reviewer if they separate from State service or have a change in employment where acting as the Agency Security Reviewer is no longer appropriate

For items 4 - 7 above, an HRIS Security Approvers/Reviewers Designation Form must be completed and submitted to HRISServiceDesk@azdoa.gov

8. Unless specifically prohibited elsewhere, an Agency Director may delegate their authority related to Agency Security Approvers/Reviewers to others in their agency.
    - This is a delegation of authority, but not of responsibility, for the actions taken by the delegate
    - All such delegations must be in writing and retained by the agency in accordance with the directives issued by Library, Archives and Public Records (LAPR)
    - Only a Director may designate a Delegate
9. Responsible for removing a Delegate if they separate from State service or have a change in employment where acting as their Delegate is no longer appropriate

For items 8 - 9 above, an HRIS Security Delegate Designation Form must be completed and submitted to HRISServiceDesk@azdoa.gov

Agency Delegates

1. Responsible for knowing and disseminating the control environment at the agency

2. Responsible for ensuring that internal controls are adhered to at the agency
3. Should have familiarity with HRIS as well as general knowledge of Human Resources, Benefits and Payroll operations at the agency
4. Responsible for designating Agency Security Approvers for the agency
    - The Delegate SHALL designate at least one employee to be authorized as an Agency Security Approver to review and approve all of the agency's user access to HRIS
5. May designate themselves as an Agency Security Approver
6. It is highly recommended that more than one Agency Security Approver is designated to ensure continuity of operations
    - Shall carefully review the qualifications of an employee who they wish to make the Agency Security Approver
    - Shall review requirements and responsibilities of the Agency Security Approver listed below
7. Responsible for removing an Agency Security Approver if they separate from State service or have a change in employment where acting as the Agency Security Approver is no longer appropriate
8. Responsible for designating Agency Security Reviewers for the agency
    - The Delegate MAY designate an employee to act as the Agency Security Reviewer to assist with managing HRIS access for its employees
    - Shall carefully review the qualifications of an employee who they wish to make the Agency Security Reviewer
    - Shall review the requirements and responsibilities of the Agency Security Reviewer listed below

9. Responsible for removing an Agency Security Reviewer if they separate from State service or have a change in employment where acting as the Agency Security Reviewer is no longer appropriate

For items 4 - 9 above, an HRIS Security Approvers/Reviewers Designation Form must be completed and submitted to HRISServiceDesk@azdoa.gov

Agency Security Approvers

1. Agency Security Approvers are **the only individuals** who may submit HRIS Security Request forms and HRIS Security ETE Proxy Request forms for the agency's employees. The HRIS Security Request forms are used to grant, change and remove HRIS access for an employee. The HRIS Security ETE Proxy Request forms are used to grant, change and remove HRIS proxy access to Employee Time Entry (ETE).
2. Responsible for reviewing and approving all of the agency's Power user and ETE Proxy access to HRIS
3. Shall not submit a request for HRIS access for themselves
    - If HRIS access is needed for themselves, the Agency Director, Agency Security Authority Delegate or ADOA Security Approver can sign and submit the security request form

4. Should be well versed in the State's HRIS system as well as have a good understanding of Human Resources, Payroll and Benefits operations and internal controls
5. Must be aware of the risks involved when the separation of duties is absent
6. Any person designated an approval authority over HRIS Security requests should:
    - Be at the level of management appropriate for such authority
    - Have the requisite operational, procedural and financial expertise to determine the appropriateness of the HRIS Security requests over which they have approval authority
7. Must be aware of factors affecting internal control such as HRIS access of each employee
8. Responsible for performing reviews of HRIS access for the agency on at least a quarterly basis
9. Upon receipt of an HRIS Security Request form or HRIS Security ETE Proxy Request form, responsible for reviewing all existing access for the employee for whom the request is being submitted to ensure compliance with the agency's internal controls
    - If upon review of existing roles and of internal controls, approving the request would cause a conflict in separation of duties, the request shall be rejected and returned to the submitting manager
    - SHALL NOT approve ETE Proxy with Approval Access to an employee who holds a security role of AgyHRGenWSSN, AgyHRGenNoSSN, ADOAPAAdmin or ADOAOrgStructure.
    - Contact the GAO Internal Audit Team at GAOInternalAudit@azdoa.gov for assistance with separation of duties questions
10. Responsible for approving HRIS Security Request forms before they are sent to the HRIS Security Team via HRISServiceDesk@azdoa.gov
11. Responsible for approving HRIS Security ETE Proxy Request forms before they are sent to the Agency ETE Proxy Administrator or Central.Payroll@azdoa.gov if Agency does not have an ETE Proxy Administrator.
12. Responsible for validating the Data Sharing Non-Disclosure Agreement Acknowledgement, Security Policy Acknowledgement and HRIS Intro course and exam in TraCorp have been completed by the employee
13. Responsible for promptly, after notification, removing HRIS access for employees if they separate from State service or have a change in employment where access to HRIS is no longer appropriate
    - An HRIS Security Request Form must be completed and submitted to HRISServiceDesk@azdoa.gov
    - An HRIS Security ETE Proxy Request Form must be completed and submitted to the Agency ETE Proxy Administrator or Central.Payroll@azdoa.gov if Agency does not have an ETE Proxy Administrator

Agency Managers and Supervisors

1. Responsible for ensuring that internal controls are adhered to at the agency

2. Should have familiarity with the HRIS System as well as general knowledge of Human Resources, Benefits and Payroll operations at the agency

3. Should understand that submitting an HRIS Security Request for an employee may allow them access to personally identifiable information (PII) or HIPAA information for employees in their agency

4. Responsible for explaining to employees who will be granted access to HRIS that any PII or HIPAA related information is confidential and sensitive data and should only be used for authorized business purposes

    - Unauthorized access and/or use of PII or HIPAA information may result in disciplinary action

1. Responsible for obtaining a Data Sharing Non-Disclosure Agreement signed by the employee

2. Responsible for advising employees which HRIS security role they will be granted and the training/exams required to obtain access to HRIS

3. Responsible for validating that employees have completed requisite training/exams with a passing grade prior to submitting the HRIS Security Request form to the Agency Security Approver

4. When an employee has a change in employment, responsible for reviewing or removing their access to Statewide Systems

    - A status change may include a change in position or duties, transfer to another agency, separation or dismissal from State service, urgent revocation of access, etc.

    - If the employee should no longer have access to HRIS, promptly inform the Agency Security Approver to remove access

Agency Security Reviewers (Optional)

1. Must be aware of factors affecting internal controls

2. Should possess at least a basic understanding of HRIS and a good understanding of internal control issues relative to separation of duties

3. Responsible for monitoring HRIS security for the agency

4. Responsible for performing reviews of HRIS access for the agency on at least a quarterly basis

5. Responsible for reporting security issues promptly to the Agency Security Approver and the Agency Director and/or Delegate

    - Reporting to all parties is required to minimize risk

1. If employee(s) have HRIS access that should be removed, responsible for contacting the employee(s)' manager/supervisor and requesting to have the HRIS Security Request form submitted immediately

Employee Time Entry (ETE) Proxy Administrators

1. ETE Security Administrators are **the only individuals** who may add ETE Proxies for the agency's employees. The HRIS ETE Proxy Request forms are used to grant, change and remove ETE Proxy access for an employee

2. Responsible for ensuring that internal controls are adhered to at the agency

3. Responsible for assigning Proxy access to employees that allows said individuals access to add, change, delete, and submit employee time records through ETE

    - ETE Proxy Request Form shall be maintained on file for each individual that is granted proxy access

4. Must be aware of factors affecting internal control such as existing HRIS access of each employee

5. Must be aware and adhere to the enforcement of separation of duties

    - The Agency ETE Proxy Administrator **SHALL NOT** assign Approval Access proxy to an employee who holds a security role of: AgyHRGenNoSSN, AgyHRGenWSSN, ADOAClassComp or ADOAPAAdmin.
    - Employee security roles are verified by the Agency Security Approver(s) on the HRIS Security ETE Proxy Request form
    - **SHALL NOT** assign proxy access for themselves

6. Any person designated an ETE Security Administrator should:

    - Be at the level of management appropriate for such authority

    - Have the requisite operational, procedural and financial expertise to determine the appropriateness of the ETE Proxy requests over which they have approval authority

7. Responsible for performing reviews of ETE Proxy access for the agency on at least a quarterly basis

8. Upon receipt of an ETE Proxy Request form, responsible for reviewing all existing access for the employee for whom the request is being submitted to ensure compliance with the agency's internal controls

- If upon review signatures are missing, the request shall be rejected and returned to the submitting Agency Security Approver

9. Responsible for promptly, after notification, removing Proxy access for employees if they separate from State service or have a change in employment where Proxy access is no longer appropriate

Agency Employees (HRIS Power Users)

1. Responsible for adhering to the internal controls set forth by the agency
2. Responsible for taking the required training and passing all exams related to their HRIS security role(s) prior to access being granted
3. Responsible for adhering to the conditions set forth in the Data Sharing Non-Disclosure Agreement located here
    - The Data Sharing Non-Disclosure Agreement is required to be on file before activating a user ID
4. Responsible for understanding that any PII or HIPAA related information is confidential and sensitive data and should only be used for authorized business purposes
    - Unauthorized access and/or use of PII or HIPAA information may result in disciplinary action.

Agency ETE Proxy (Assigned by ETE Proxy Administrators)

1. Responsible for adhering to the internal controls set forth by the agency
2. Responsible for taking the required training and passing all exams related to their HRIS security role(s) prior to access being granted
3. Responsible for adhering to the conditions set forth in the Data Sharing Non-Disclosure Agreement located here
    - The Data Sharing Non-Disclosure Agreement is required to be on file before activating a user ID
1. Responsible for understanding that any PII or HIPAA related information is confidential and sensitive data and should only be used for authorized business purposes
    - Unauthorized access and/or use of PII or HIPAA information may result in disciplinary action.

ADOA HRIS Security Administration Responsibilities

HRIS Security Team

1. Responsible for updating and maintaining a list of agency Directors, Delegates, Security Approvers and Security Reviewers

2. Responsible for verifying HRIS security request forms are submitted by the appropriate agency staff and the forms are complete and accurate

    - All HRIS security request forms must be submitted by the Agency Security Approver

3. Responsible for verifying the Data Sharing Non-Disclosure agreement is on file before activating a user ID

4. Responsible for creating user IDs and assigning the requested security role(s) to that user ID in HRIS, Data Warehouse, Talent Management and MAP (if applicable)

5. Responsible for validating security roles assigned to an employee will not conflict with the separation of duties matrix located at https://hr.az.gov/HRIS-Security

6. Responsible for validating that employees have completed requisite training with a passing grade prior to granting access into HRIS

7. If any request does not meet the stated requirements it will be rejected and returned to the agency

8. Responsible for disabling access when notified that an employee has terminated or retired

9. Responsible for deleting Power User accounts that have been idle for 90 days or more and notifying the HRIS Help Desk of idle Power User accounts that were deleted

10. If HRIS access abuse is discovered (sharing user ID/password, actions performed not relevant to job duties, etc.), HRIS Security is responsible for notifying the Agency Security Approver(s), Director and Delegate(s) and the HRIS Manager so appropriate action can be taken by the agency and HRIS leadership.